Cost Effective Use of Formal Methods in V&V

D. Richard Kuhn
Ramaswamy Chandramouli
National Institute of Standards and Technology
Gaithersburg, MD 20899

Ricky W. Butler
NASA Langley Research Center
Hampton, VA

National Institute of Standards and Technology
NIST
...working with industry to develop and apply technology, measurements and standards

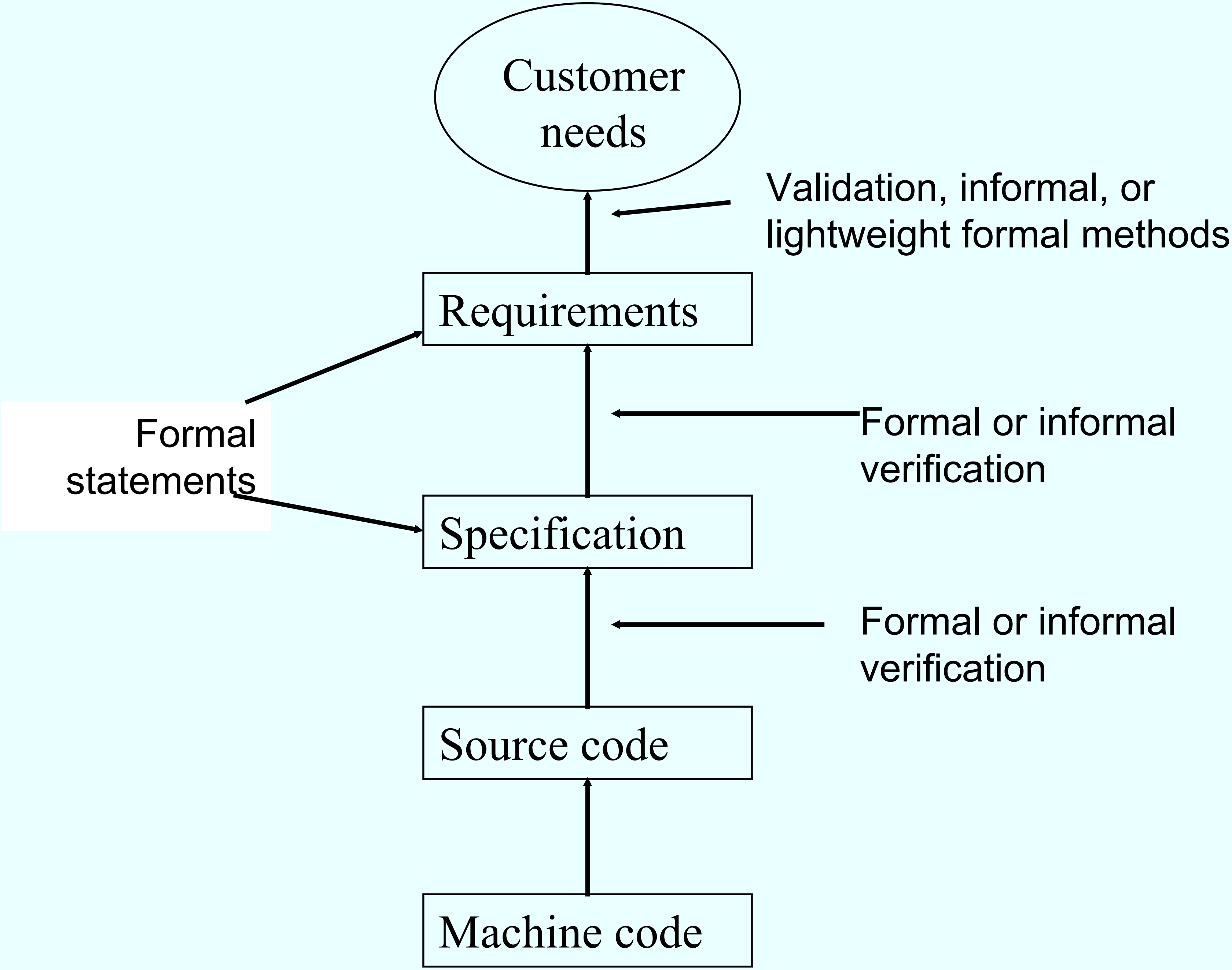
NASA

The Problem

If attainable, a formal proof of correctness is the most effective means of model V&V. Unfortunately, "if attainable" is the sticking point. Current formal proof of correctness techniques cannot even be applied to a reasonably complex simulation; however, formal techniques can serve as the foundation for other V&V techniques [DMSO, 2001]

Cost Effective Uses of Formal Methods

- “Traditional” formal methods
  - design verification
  - algorithm/code verification
- New applications
  - “lightweight” formal methods - requirements validation
  - test case generation
- When and where do these methods make sense?


Customer needs

Validation, informal, or lightweight formal methods

Requirements

Formal statements

Formal or informal verification

Specification

Formal or informal verification

Source code

Machine code

Improving Precision in Specifications

- Most fundamental requirement for any V&V - precise specification
- Formalizing spec may be most valuable part of formal verification
  - reveal ambiguities, omissions
  - improve communications between developers and customers
  - vital for component based software
  - avoid “bring me a rock” development

Analyzing and Proving Properties of Systems and Specifications

- System requirements and behavior stated in some formal logic
  - first order predicate calculus
  - temporal logic
  - propositional calculus
- Can then be analyzed with automated tools

Theorem Proving Tools

- Fully general, accepting specifications in wide variety of logics
- Require human intervention
- Most powerful analysis tools, but require most skill to run
- Many built-in heuristics to make use easier

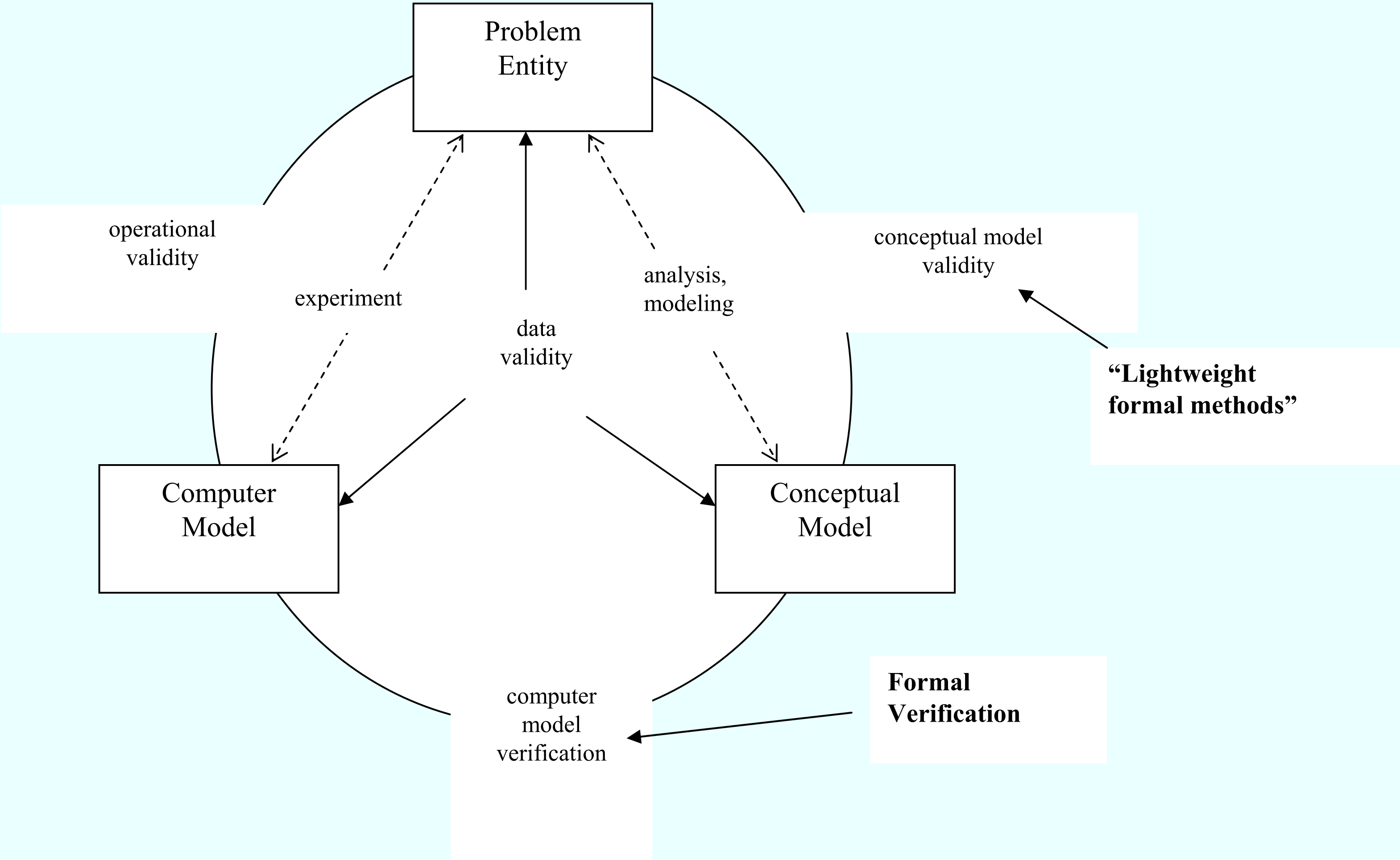
Model Checkers

- Accept finite state model of system
- Automatically verify certain properties:
  - correct event sequence
  - proper consequences of activities
  - simultaneous occurrence of events
  - mutual exclusion of events
  - required precedence
- Less skill required, but more limited application (although apply to real systems)

Using Formal Techniques in Validation

- “Lightweight formal methods”
- Analyze properties to determine if “building the right system”
- Used interactively with customers
- For M&S systems, probably most useful for “conceptual model validation” - analyzing assumptions, logic, and structure

Lightweight Formal Methods in Modeling & Simulation



Problem Entity

Computer Model

Conceptual Model

operational validity

experiment

data validity

analysis, modeling

conceptual model validity

computer model verification

“Lightweight formal methods”

Formal Verification

Can Formal Methods be used in Certification Standards?

- Early experience - DoD Trusted Computer Security Evaluation Criteria
  - formal specification and proof required at highest level (A1)
  - good tools developed
  - a few A1 systems developed for government customers

Cost and Practicality of Mandating Formal Methods

"The requirements in the current Criteria, coupled with the costly evaluation process, have led many vendors to conclude that it is simply not worth the effort to develop systems at those levels where formal methods are required." [Denning, 1999]

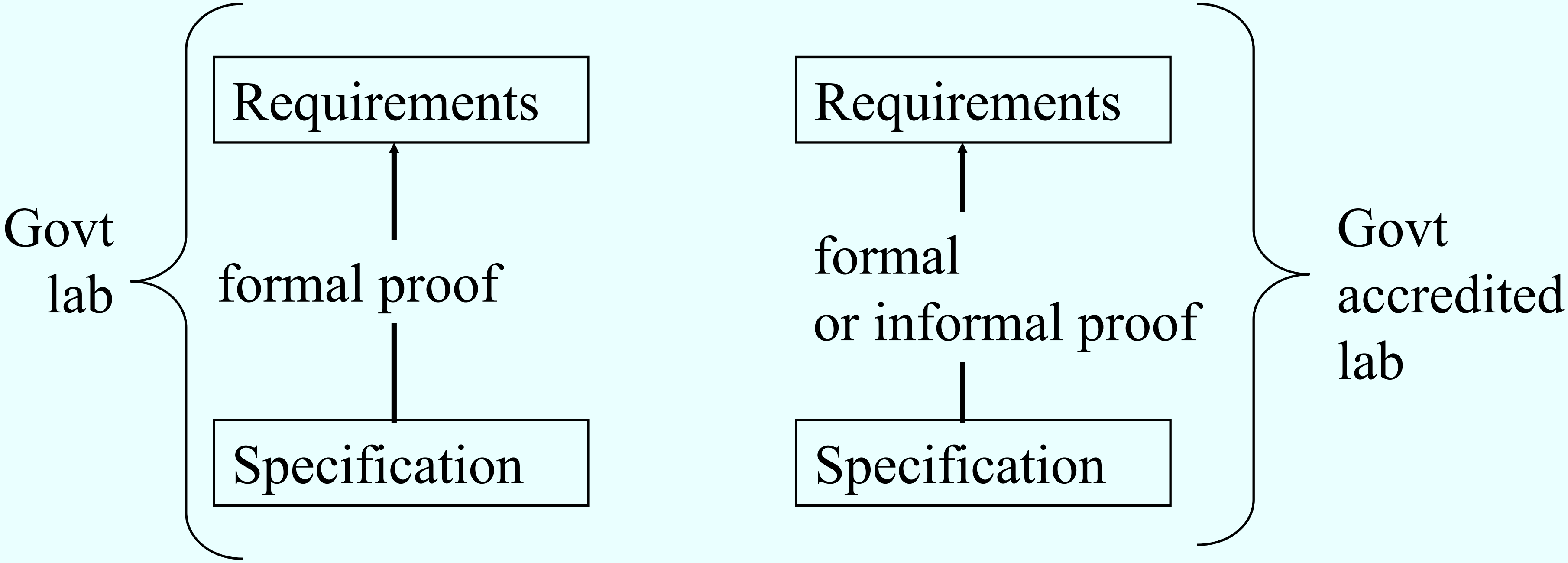
Why High Level TCSEC Systems not Worth the Effort?

- Formal processes required:
  - formal policy model/requirements
  - formal top level specification
  - full machine checked proof
- Long evaluation process
  - one lab
  - by the time a product evaluated, it was obsolete [Lipner, 1991]

Implications of TCSEC Experience

- If a standard requires formal methods, must be at a level for which there is large market
  - additional development cost 10% - 15%
- Formal methods requirements must not significantly increase time to market
  - evaluation must be shorter than one release cycle
  - evaluation market must grow with product market

Applying Lessons Learned - FIPS 140-1 Crypto Module Std



TCSEC

FIPS 140-1

FIPS 140-1 Results

- Basic formal methods required at all levels
  - over 200 products evaluated
  - independent training courses specifically for FIPS 140-1 process
- Strong formal methods requirements at highest level
  - 8 products, more than any other standard
  - all for commercial advantage, not govt contract

Suggested Implications for M&S

- Formal methods for certified components
  - large market
  - third-party evaluation labs appropriate
- “Lightweight formal methods” for requirements validation
- Automated test generation for one-of-a-kind systems

Estimated Costs of Automated Test Generation Under Conservative Assumptions

	Traditional	Formal spec & verification w/out test generation	Formal spec & verification w/ test generation (a)	Formal spec w/ test generation (b)	Formal spec with test generation (c)
Design, code, other costs	50%	50%	50%	50%	50%
Test coding	30%	30%	15%	15%	10%
Test execution	20%	20%	20%	20%	20%
Formal specification	---	10%	10%	10%	10%
Formal verification	---	10%	10%	---	---
Cost compared to traditional		120%	105%	95%	90%